CONVERSATION CASE

Privacy, Surveillance, and Self-Disclosure

What is a reasonable expectation of privacy in the context of teens’ online lives? What roles should schools play in monitoring social media? Who should teens expect might look at their online posts, and how can they sufficiently protect themselves? This case focuses on the role of schools related to tracking students’ social media posts. In the wake of tragic incidents of cyberbullying and a mix of other social media-fueled issues, schools are grappling with how best to protect and support their students. For many districts, questions of whether and how to monitor the “online playground” — and even how to avoid liability — loom large.

Key Vocabulary

<table>
<thead>
<tr>
<th><strong>post</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>A post is content — text, a picture, a link — shared online for others to see. Posts can take the form of “tweets” on Twitter or “status updates” on Facebook.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Twitter</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Twitter is a microblogging site that allows users to post brief, 140-character messages — called “tweets” — and follow other users’ activities. Teens like using Twitter to share quick tidbits about their lives with friends. It’s also great for keeping up with what’s going on in the world — breaking news, celebrity gossip, etc.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>privacy settings</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy settings allow users some control over what information is shared and with whom. However, many platforms require that users actively seek out and set their privacy settings; default settings are often the most lenient or public.</td>
</tr>
</tbody>
</table>
The Case, Part 1: School Surveillance

The following excerpts are from an article titled “Warily, Schools Watch Students on the Internet.” The article appeared in The New York Times on October 28, 2013.

SAN FRANCISCO — For years, a school principal's job was to make sure students were not creating a ruckus in the hallways or smoking in the bathroom. Vigilance ended at the schoolhouse gates.

Now, as students complain, taunt and sometimes cry out for help on social media, educators have more opportunities to monitor students around the clock. And some schools are turning to technology to help them. Several companies offer services to filter and glean what students do on school networks; a few now offer automated tools to comb through off-campus postings for signs of danger. For school officials, this raises new questions about whether they should — or legally can — discipline children for their online outbursts.

The problem has taken on new urgency with the case of a 12-year-old Florida girl who committed suicide after classmates relentlessly bullied her online and offline.

Two girls — ages 12 and 14 — who the authorities contend were her chief tormentors were arrested this month after one posted a Facebook comment about her death. Although the charges were later dropped, the case helped to shine light on a very important issue.

Educators find themselves needing to balance students’ free speech rights against the dangers children can get into at school and sometimes with the law because of what they say in posts on Facebook, Twitter and Tumblr. Courts have now started to weigh in.

In September, a federal appeals court in Nevada, for instance, sided with school officials who suspended a high school sophomore for threatening, through messages on Myspace, to shoot classmates. In 2011, an Indiana court ruled that school officials had violated the Constitution when they disciplined students for posting pictures on Facebook of themselves at a slumber party, posing with rainbow-colored lollipops shaped like phalluses.

“It is a concern and in some cases, a major problem for school districts,” said Daniel A. Domenech, executive director of the American Association of School Administrators, which represents public school superintendents. Surveillance of students’ online speech, he said, can be cumbersome and confusing. “Is this something that a student has the right to do, or is this something that flies against the rules and regulations of a district?”

Interviews with educators suggest that surveillance of students off campus is still mostly done the old-fashioned way, by relying on students to report trouble or following students on social networks. Tracking students on social media comes with its own risks: One principal in Missouri resigned last year after accusations that she had snooped on students using a fake Facebook account. “It was our children she was monitoring,” said one Twitter user who identified herself as Judy Rayford, after the news broke last year, without, she added, “authorization” from children or parents.
But technology is catching on. In August, officials in Glendale, a suburb in Southern California, paid Geo Listening, a technology company to comb through the social network posts of children in the district. The company said its service was not to pry, but to help the district, Glendale Unified, protect its students after suicides by teenagers in the area.

Students mocked the effort on Twitter, saying officials at G.U.S.D., the Glendale Unified School District, would not “even understand what I tweet most of the time, they should hire a high school slang analyst #shoutout2GUSD.”

“We should be monitoring gusd instead,” one Twitter user wrote after an instructor was arrested on charges of sexual abuse; the instructor pleaded not guilty.

Chris Frydrych, the chief executive of Geo Listening, based in Hermosa Beach, also in Southern California, declined to explain how his company’s technology worked, except to say that it was “a sprinkling of technology and a whole lot of human capital.” He said Geo Listening looked for keywords and sentiments on posts that could be viewed publicly. It cannot, for instance, read anyone’s Facebook posts that are designated for “friends” or “friends of friends.”

But with Facebook’s announcement this month that teenagers will be permitted to post public status updates and images, Geo Listening and similar services will potentially have access to more information on that social network.

Glendale has paid Geo Listening $40,500 to monitor the social media posts. Mr. Frydrych declined to say which other schools his company works with, except to predict that by the end of the year his company would have signed up 3,000 schools.

David Jones of CompuGuardian, based in Salt Lake City, said his product let school officials monitor whether students were researching topics like how to build bombs or discussing anorexia. His customers include five schools, but he too, is optimistic about market growth. “It helps you boil down to what students are having what problems,” he said. “And then you can drill down.”

**But when does protecting children from each other or from themselves turn into chilling free speech? (...)**

(...) That fine line seems to be equally confounding the courts.

In the Nevada case, a 16-year-old boy bragged on Myspace about having guns at home, and threatened to kill fellow students on a particular date. He also cited the 2007 massacre at Virginia Tech, in which a troubled student killed 32 people.

The boy ended up spending 31 days in a local jail and was suspended from school for 90 days. He then sued the district, saying his free speech rights had been violated.

The Ninth Circuit Court of Appeals dismissed the claim. It called his threats “alarming” and so specific that they presented “a real risk of significant disruption” to the school. Administrators were justified, the court ruled, for penalizing what was ostensibly off-campus speech.
“It’s going to be more and more of legal issues,” said Gretchen Shipley, a lawyer who represents school districts. “The ability to monitor is growing so quickly.”

The Indiana case offers a contrast. In the summer of 2009, two incoming 10th graders at Churubusco High School posted what the court called “raunchy” pictures of themselves. Once school officials found out, the girls were suspended from extracurricular activities for the school year. The girls sued, saying their free speech rights had been violated. The school contended that its student handbook bars conduct that could “discredit” or “dishonor” it.

The court found that prohibition too broad. The students’ pictures, “juvenile” though they were, did not cause “substantial disruption” at school, the court ruled, and even though it was just “crude humor,” it was protected speech. “No message of lofty social or political importance was conveyed, but none is required,” the court said.

The full article can be accessed at: [http://nyti.ms/1b1BGUO](http://nyti.ms/1b1BGUO)

**Consider**

- What surprises or concerns you about this story?
- What are the pros and cons of schools monitoring students’ social media? Where do you fall on the debate?
- Are there alternative ways schools can support students regarding their social media lives?
- What do you think the school’s motivations were for hiring Geo Listening? Do you think the approach will have the intended impact?
- How would you feel — relieved, angry, nervous, apathetic — if your school district started monitoring your child’s social media posts?
- Does it make a difference what kind of information the sites are looking for or collecting?
- How do you think about your child’s online privacy? Who should information be private from? What information should stay private – and what does it mean to keep it private?


Azzam, Twitter post, October 22, 2013. 7:15 p.m.
[https://twitter.com/search?q=%23shoutout2GUSD&src=hash](https://twitter.com/search?q=%23shoutout2GUSD&src=hash)

Gahribian, Michael, Twitter post, October 17, 2013. 8:36 p.m.
[https://twitter.com/MichaelGhar/status/391045030929899520](https://twitter.com/MichaelGhar/status/391045030929899520)

Rayford, Judy, Twitter post, May 7, 2012. 1:15 p.m.
[https://twitter.com/jcr_each/status/19959354122633216](https://twitter.com/jcr_each/status/19959354122633216)

Online privacy is tricky. The information that we put in digital form can now be readily accessed by unintended viewers, whether because of an oversight in selecting privacy settings, the vulnerability of “secure” online data, sharing passwords that grant others access to personal accounts, or simply because a friend’s eyes wander to read personal text messages. Work together with your kids to be vigilant about keeping private information private.

- **Underscore that any digital information has the potential to go public.**
  Information posted online or shared digitally (a picture, a status update, a text message) is searchable, easily copied, and often permanent. Even if your kids set strict privacy settings, there is the chance that a friend could copy/paste, take a screenshot, save, or forward something your kid didn’t want to get widely shared. Or, a curious onlooker may simply steal a glimpse at their screens and read private messages. Password sharing with friends, while often done causally, leads to serious privacy issues and should be avoided. Make sure your kids know that it is their responsibility to set privacy settings thoughtfully and to keep passwords private - but also remind them that anything shared digitally might be seen by unintended audiences.

- **Together, set privacy settings on all social media accounts.**
  On a daily basis, you and your children probably use different apps and sites. Together, explore how varied privacy settings and privacy policies are. Discuss how companies use their members’ personal information, and urge your children to be responsible and use “friends only” privacy settings. Many social media platforms default to mostly “public” settings — requiring users to set privacy controls. And many sites frequently require updates, which reset all settings back to the default. Not only will these opportunities help safeguard you and your children, but you will get insight into how and why your child participates in the digital world.

- **Be patient and take the time to understand all the features.**
  While companies don’t always make it easy to understand their privacy settings and privacy policies, take the time to dig in. Be wary of “social sign-in” (like using your Facebook or Twitter login to sign onto other sites), because that entitles third parties to collect data from your accounts. Set privacy settings for each and every type of content — profile information, posts, comments, and photos. And learn what individual features do, like tagging and blocking, to help you and your children manage and control your presence online. If your kid’s school provides devices, it may have the right — and responsibility — to monitor all content on the machines. Make sure your children know that they can’t assume their digital life is private from you or from anyone else.
DIGITAL DILEMMA

Privacy, Surveillance, and Self-Disclosure

Digital Dilemmas are brief hypothetical situations and corresponding questions designed to foster cross-generational conversations about different aspects of adolescents’ digital lives. Use this fictitious scenario, based on real-life stories, to spark a conversation at home with your children and open up the discussion about these very important topics.

Breaking and Entering

Nik and his girlfriend Blair were hanging out at his house. Blair got up to go to the bathroom and left her phone on the couch. While she was gone, Nik noticed her phone light up and saw the name Matthew out of the corner of his eye. He was torn about whether or not to look, but decided he would just take a quick look at the texts that he could see on the main screen. Then, he couldn’t resist: he knew her phone password, so he typed it and opened the conversation. Before he knew it, he was scrolling through Blair’s conversations. He saw that she had been texting Matthew a lot. Nik was furious, but he couldn’t decide whether or not to confront Blair and admit that he had looked at her text messages. Finally, he decided he was too angry to ignore it. Blair could not believe that Nik had looked through her messages — she thought that he trusted her and she felt like this was a complete invasion of her privacy.

What is your gut reaction to this story?

Can you understand Nikhit’s decision to read Blair’s text messages? Has there ever been a situation when you wanted to read someone’s messages?

What do you think about Blair’s reaction: Did she have a right to be angry?

Are there any situations when it is okay to read another person’s private messages or emails?

Have you ever heard of something like this happening to someone you know? Has it ever happened to you?